2004

NASA FACULTY FELLOWSHIP PROGRAM

MARSHALL SPACE FLIGHT CENTER

THE UNIVERSITY OF ALABAMA
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE
ALABAMA A&M UNIVERSITY

RELIABILITY ASSESSMENT OF CONCEPTUAL LAUNCH VEHICLES

Prepared By:	Lisa A. Bloomer
Academic Rank:	Assistant Professor
Institution and Department:	Middle Tennessee State University Department of Mathematical Sciences
NASA/MSFC Directorate:	Safety and Mission Assurance
MSFC Colleague:	Vyga Kulpa

Introduction

Planning is underway for new NASA missions to the moon and to MARS. These missions carry a great deal of risk, as the Challenger and Columbia accidents demonstrate. In order to minimize the risks to the crew and the mission, risk reduction must be done at every stage, not only in quality manufacturing, but also in design. It is necessary, therefore, to be able to compare the risks posed in different launch vehicle designs. Further, these designs have not yet been implemented, so it is necessary to compare these risks without being able to test the vehicles themselves.

This paper will discuss some of the issues involved in this type of comparison. It will start with a general discussion of reliability estimation. It will continue with a short look at some software designed to make this estimation easier and faster. It will conclude with a few recommendations for future tools.

Risk and Reliability

Risk and reliability are very closely related. Risk is defined as the probability that a system will fail, and reliability is the probability that it will perform as designed. So, risk is a number that is hopefully close to zero, reliability is a number close to one, and they are related in that reliability is one minus risk.

Because the reliability of a system is unknown, it is necessary to estimate it. If the system has already been designed and built in large numbers, it is a straightforward statistical exercise to estimate the reliability. Simply test the system many times, and estimate the reliability as the number of times the systems performed as designed, divided by the total number of trials. This number is referred to as *demonstrated reliability*.

Point estimates of reliability can be misleading. For example, if a system is tested 1000 times with no failures, the point estimate is that the system is 100% reliable. But this estimate does not match reality – no system is 100% reliable. It is useful to provide an interval estimate instead. So, if a system is tested 1000 times with no failures, we can say with 95% confidence that the reliability is somewhere between 0.997 and 1. A more common statement is that the reliability is 0.997 with 95% confidence. This is just an abbreviation. One way to interpret the confidence level is that the probability that the reliability is in the specified interval is 0.95 – that is, that there is a 5% chance of an error. The confidence level, paired with the width of the interval, is an indication of uncertainty. A system that has been tested ten thousand times will have a shorter confidence interval at the same confidence level than one that was tested one thousand times.

A goal articulated by the Astronaut Office is that the reliability for crewed vehicles should be 0.999 with 95% confidence. That is, the risk of a member of the crew dying should be less than 1 in 1000, with a less than 5% chance that the risk is greater. To verify that level of reliability, the launch vehicle would have to be tested 2995 times with no failures. This level of testing is highly unlikely for a system so complex and expensive. The Space Shuttle, for example, has flown 113 missions. Furthermore, the system was modified several times, so combining those missions into one demonstrated reliability number is statistically suspect.

Estimating reliability in another way – by testing at a component level and calculating system reliability as a function of the component reliabilities – yields a number called *predicted reliability*. For example, if a system consists of two components, both of which must function for the system to function, and the components each have a reliability of 0.99, then the system reliability is 0.99*0.99=0.9801. Finding the predicted reliability of a more complex system requires detailed knowledge about how the system works. This knowledge can be summarized in fault trees or other diagrams which can then be used to make the calculation of predicted reliability easier.

As with demonstrated reliability, predicted reliability is more useful if it is reported in terms of confidence intervals rather than point estimates. Tracking how the confidence level is affected by the combination of estimates is difficult. For example, if a system has two components whose reliability are estimated at a 95% level, and the components are manufactured independently of each other, the system's confidence level is greater than 0.95*0.95=0.9025, and less than 1-0.05*0.05=0.9975. But this range is quite large, and different assumptions about the components and their interrelation in the system yield different values for the confidence level of the system. Because this problem is complicated, it is common to use simulation to estimate the predicted reliability. This will be discussed further in the next section.

Demonstrated and predicted reliability numbers are both estimates of an underlying reliability which is unknown. In fact, however, they measure different quantities. Demonstrated reliability gives the reliability of a system as built and tested. That is, it is affected not only by the design of the system, but also by the quality of the manufacturing process, any issues in storage and transport, and the variables (such as temperature and human factors) introduced during testing. The uncertainty of demonstrated reliability number is mainly affected by the number of tests run. Predicted reliability, on the other hand, is based on the design of the system and any assumptions about other factors affecting reliability. For example, guidelines for the reporting of figures of merit during a conceptual study of launch vehicles allow the assumption that the software running the system is 100% reliable. Also, predicted reliability numbers will, by the nature of the calculations, not include unanticipated risks. Therefore, there are more sources of uncertainty in a predicted reliability number. However, in a system that has only been tested a few times, the demonstrated reliability will be highly uncertain and the predicted reliability may be more certain. This may lead to the two numbers being combined in a weighted average that takes into account the relative uncertainties.

Reliability Software

The predicted reliability of systems is often estimated using simulation. Usually, the risk of a failure in a particular component is calculated, taking into account variables such as the age of the component, temperature, etc. Then, using this risk, a randomized decision is made as to whether that component failed. The consequences of such a failure are tracked using event sequence diagrams, and a notation is made if the failure of the component resulted in the failure of the system. This process is repeating a large number of times, and the proportion of times the system failed is reported. By varying the values of the input variables according to probability distributions that reflect uncertainty, many different estimates for system reliability can be made. Then a 95% confidence interval for system reliability can be estimated by, for example, making the upper endpoint 1 and the lower endpoint the 5th percentile of the simulated reliabilities.

The Flight-oriented Integrated Reliability and Safety Tool (FIRST) was developed by Science Applications International Corp (SAIC) to predict the reliability of launch vehicles through several figures of merit: the probability of Loss of Vehicle (LOV), Loss of Payload (LOP), and Loss of Mission (LOM). Loss of Crew (LOC) is also included, but the definition of this figure of merit has not yet been agreed upon by all the stakeholders, so it may have to be changed. FIRST started as an Excel and Crystal Ball model. A user interface has been added and capabilities increased. FIRST also contains reliability information about many components of launch vehicles. The current version is FIRST 2.7.3, with version 2.8 to be released shortly.

The main strength of FIRST is that it speeds up the analysis of launch vehicles, which allows several conceptual configurations to be compared. FIRST has also been used to determine the effects of design decisions. For example, the decision to add an engine to allow for recovery if one engine fails (an "engine-out capability") involves the tradeoff of increased weight, possibly increasing the number of flights needed to accomplish a mission, versus the ability to recover from an engine failure. Quantifying what happens to the LOM figure with and without engine-out capability helps with these decisions.

FIRST was designed to be used by SAIC analysts who understand the estimation process as well as the inner workings of the software. It should therefore be run by someone with a lot of reliability experience and training in the software. It should also be mentioned that the reliability information that FIRST contains for the various engines and other components each come from different NASA sources and have not been vetted as a group. Some components – types of engines, for example – are not included, and there is no simple way to add in a conceptual component. FIRST 2.7.3 does not easily allow for multistage craft, but this should be added in FIRST 2.8.

There are other software packages available for reliability analysis. Failure Environment Analysis System – MSFC (FEAS-M) is a physics based system that allows the user to create trees describing the relationships between different variables and then simulate. FEAS-M was developed at Marshall Space Flight Center. Quantitative Risk Assessment System (QRAS) was developed at NASA and is currently being maintained by the University of Maryland. It was used to perform a probabilistic risk assessment of the Space Shuttle Program a few years ago. Defect Detection and Prevention (DDP) is a software package designed by the Jet Propulsion Laboratory to manage implementation of a reliability system from design through manufacturing.

Commercial software is also available. The spreadsheet Excel and the simulation add-in Crystal Ball are powerful for their flexibility. The company Reliasoft has several reliability packages available for different types of analysis. And Relex also has several software packages that do reliability analysis.

FIRST fills a specific niche in the analysis of launch vehicles. The other software packages are general and can implement this type of analysis, but are not already set up to do so. Also, the data about component reliability that are stored within FIRST would have to be easily accessed to use these packages. It should be emphasized that predicted reliability estimates from one package should not be closely compared to those from another package. This is because it is highly unlikely that the two models used the same assumptions. If it becomes necessary to do such a comparison, effort should be made to identify differing assumptions.

Conclusion

The estimation of the risk and reliability of launch vehicles is an important task, especially coming when the vehicles are still at a conceptual stage. This allows designs to compete not only on a basis of cost and feasibility, but also on risks posed to the crew and the mission. There are two types of estimated reliability, demonstrated and predicted reliability. If the system has not yet been built, it is impossible to calculate demonstrated reliability and it becomes necessary to predict reliability based on that of the components of the system.

Various software packages are available for this estimation process. FIRST is designed for the analysis of launch vehicles, while other software packages are available for more general tasks. All of the software requires the user to be knowledgeable about reliability analysis as well as the system being analyzed.

An important component of the process of estimating reliability for a system based on the reliability of the components is to have a database of components available. These data should contain the best available information on each component as well as estimates for the certainty of the information stored.

References

[1] "Astronaut Office Position on Future Launch System Safety," LMA Correspondence Control # 04-AST-00013, May 4, 2004.

[2] Birolini, A. Reliability Engineering: Theory and Practice, 3rd edition. Springer, NY 1999.

[3] Rausand, M. and Høyland, A. System Reliability Theory: Models, Statistical Methods, and Applications, 2nd edition. Wiley, NJ 2004.